IFW

FORM PTO-1083

PATENT
Case Docket No. MEI-101

In RE application of Y. ISHII et al.
Serial No.: 10/786,072
Filed: February 26, 2004

Group Art Unit: 2161
Examiner: S. METJAHIC

For: EMERGENCY ACCESS INTERCEPTION ACCORDING TO BLACK LIST

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Transmitted herewith is an Amendment in the above-identfied application.

□ Small entity status of this application under 37 CFR 1.9 and 1.27 has been established by a verified statement previously submitted.

□ A verified statement to establish small entity status under 37 CFR 1.9 and 1.27 is enclosed.

□ No additional fee is required.

The fee has been calculated as shown below:

	(COL. 1)		(COL. 2)	(COL. 3)
▨	Claims Remaining After Amendment	▨	Highest No. Previously Paid For	Present Extra
Total	• 23	Minus	•• 23	= 0
Indep.	• 9	Minus	••• 9	= 0
□ First Presentation of Multiple Dependent Claims				

SMALL ENTITY

Rate	Additional Fee
x 9	$
x 42	$
+ 140	$
Total	$

OR

OTHER THAN A SMALL ENTITY

Rate	Additional Fee
x 18	$ 0
x 84	$ 0
+ 280	$ 0
Total	$ 0

OR

• If the entry in Col. 1 is less than the entry in Col. 2, write '0' in Col. 3.
•• If the 'Highest Number Previously Paid For' IN THIS SPACE is less than 20, write '20' in this space.
••• If the 'Highest Number Previously Paid For' IN THIS SPACE is less than 3, write '3' in this space.
The 'Highest Number Previously Paid For' (Total or Independent) is the highest number found from the equivalent box in Col. 1 of a prior Amendment or the number of claims originally filed.

□ Please charge my Deposit Account No. 50-1417 in the amount of $________.

☒ A check in the amount of $ 130.00 is attached in payment of: CREDIT CARD FORM FOR PETITION TO MAKE SPECIAL FEE. .

☒ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 50-1417.

- ☒ Any filing fees under 37 CFR 1.16 for the presentation of extra claims.
- ☒ Any patent application processing fees under 37 CFR 1.17.
- ☒ Any Extension of Time fees that are necessary, which are hereby requested if necessary.

MATTINGLY, STANGER & MALUR, P.C.
1800 Diagonal Rd., Suite 370
Alexandria, Virginia 22314
(703) 684-1120

By: Daniel J. Stanger
Registration No. 32,846
Attorney for Applicant(s)

Date: July 29, 2005

MEI-101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Y. ISHII, et al.		
Serial No.:	10/786,072	Group Art Unit:	2161
Filed:	February 26, 2004	Examiner:	Safet METJAHIC
For:	EMERGENCY ACCESS INTERCEPTION ACCORDING TO BLACK LIST		

PETITION TO MAKE SPECIAL UNDER 37 CFR §1.102(MPEP §708.02(VIII))

MS Petition
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

July 29, 2005

Sir:

Applicants hereby petition the Commissioner to make the above-identified application special in accordance with 37 CFR §1.102(d). Pursuant to MPEP §708.02(VIII), Applicants state the following.

(A) This Petition is accompanied by the fee set forth in 37 CFR §1.17(h).

The Commissioner is hereby authorized to charge any additional payment due, or to credit any overpayment, to Deposit Account No. 50-1417.

(B) All claims are directed to a single invention.

If the Office determines that all claims are not directed to a single invention, Applicant will make an election without traverse as a prerequisite to the grant of special status in conformity with established telephone restriction practice.

(C) A pre-examination search has been conducted.

The search was directed towards a storage system. In particular, the search was directed towards an access controller, method for access control, and computer program as claimed in the independent claims discussed below, that controls an access to an information resource stored in a storage device connected via a network to a plurality of access controllers and storage devices.

As claimed in independent claim 1, an access controller comprises an access restriction module configured to restrict access to each information resource according to an access control list, an access interception module configured to intercept an access by an access prohibited user listed on an access prohibition list, an input module configured to input user information, and a list update module configured to update the access prohibition list according to the user information input through the input module.

As claimed in independent claim 9, an access controller comprises an access restriction module configured to restrict access to each information resource according to an access control list, a receiving module configured to receive user information of an access prohibited user from another access controller, a list update module configured to update an access prohibition list, and an access interception module configured to restrict the access by reference to the access prohibition list prior to the access control list.

As claimed in independent claim 15, in which a plurality of storage devices for storing information resources and access controllers for controlling accesses to the information resources are connected with a network, each access controller comprises an access restriction module configured to restrict access to each information resource according to an access control list, and an access interception module configured to restrict the access by reference to an access prohibition list, wherein at least one of the access controllers corresponding to the updated access prohibition list further comprises a distribution module configured to send out the user information or the updated access prohibition list to another access controller in response to the update, and the other access controller further comprises a list update module configured to receive the user information or the updated access prohibition list and to update the access prohibition list of the other access controller.

As claimed in claim 18, in which a plurality of storage devices for storing information resources and access controllers for controlling an access to the information resources are connected with a network, each access controller comprises an access restriction module configured to restrict access to each information resource according to an access control list, an access interception module configured to restrict the access by reference to an access prohibition list, a distribution module configured to broadcast the user information to another access controller in response to update of the access controller's own access prohibition list, a list update module configured to update the access controller's own access prohibition list, an access control list update module configured to update the access control list according to the user information after updating the access prohibition list, and a user information deletion module configured to delete the user information from the access prohibition list after updating the access control list.

As claimed in independent claim 19, a method for controlling an access to an information resource stored in a storage device, the method being executed by an access controller in a system where a plurality of the access controllers and the storage devices are connected with a network, comprises the steps of restricting access to each information resource according to an access control list on which an access right to each information resource is recorded, intercepting an access by an access prohibited user listed on an access prohibition list, inputting user information corresponding to the access prohibited user, and updating the access prohibition list corresponding to each access controller connected with the network, according to the input user information.

As claimed in claim 20, a method for controlling an access to an information resource stored in a storage device, the method being executed by an access controller in a system where a plurality of the access controllers and the storage devices are connected with a network, comprises the steps of restricting access to each information resource according to an access control list on which an access right to each information resource is recorded, receiving user information of an access prohibited user from another access controller, updating an access prohibition list on which user information of access prohibited users is recorded, according to the received user information, and restricting the access by reference to the access prohibition list prior to the access control list.

As claimed in claim 21, a method for controlling an access to information resources in an access control system where a plurality of storage devices for storing information resources and access controllers are connected with a network, comprises that each access controller restricts access to each information resource according to an access control list, each access controller restricts the access by reference to an access prohibition list, at least one of the access controllers corresponding to the updated access prohibition list sends out the user information or the updated access prohibition list to another access controller in response to the update, and the other access controller receives the user information or the updated access prohibition list and updates the access prohibition list of the other access controller.

As claimed in claim 22, a computer readable recording medium contains a computer program executed by an access controller to control an access to an information resource stored in a storage device, the computer program being executed in a system where a plurality of the access controllers and the storage devices are connected with a network, the computer program comprising a first program code for restricting access to each information resource according to an access control list on which access right to each information resource is recorded, a second program code for intercepting an access by an access prohibited user listed on an access prohibition list, a third program code for inputting user information corresponding to the access prohibited user, and a fourth program code for updating the access prohibition list corresponding to each access controller connected with the network, according to the input user information.

Finally, as claimed in claim 23, a computer readable recording medium contains a computer program executed by an access controller to control an access to an information resource stored in a storage device is stored, the computer program being executed in a system where a plurality of the access controllers and the storage devices are connected with a network, the computer program comprising a first program code for restricting access to each information resource according to an access control list on which access right to each information resource is recorded, a second program code for receiving user information of an access prohibited user from other access controller, a third program code for updating an access prohibition list on which user information of access prohibited users is recorded, according to the received user information, and a fourth program code for restricting the access according to the access prohibition list prior to the access control list.

The search of the above features was conducted in the following areas:

Class	Subclass
707	9
709	225, 229
711	111, 112, 114, 163
713	182, 200, 201

Additionally, a computer database search was conducted on the USPTO Examiner Application Search Tool (EAST). Furthermore, a non-patent literature search was performed on the Association for Computing Machinery (ACM) online databases.

(D) The following is a list of the references deemed most closely related to the subject matter encompassed by the claims:

U.S. Patent Number	Inventors
6,772,350	Belani, et al.

U.S. Patent Publication No.	Inventor(s)
2002/0053029	Nakamura, et al.
2002/0138727	Dutta, et al.
2003/0028798	Burnett
2004/0127190	Hanson, et al.
2005/0065935	Chebolu, et al.

A copy of each of these references is enclosed in an accompanying IDS.

(E) It is submitted that the present invention is patentable over the references for the following reasons.

It is submitted that the cited references, whether taken individually or in combination with each other, fail to teach or suggest the invention as claimed. In particular, the cited references, at a minimum, fail to teach or suggest in combination with the other limitations recited in the claims:

a first feature of the present invention as recited in independent claim 1, wherein an access interception module is configured to intercept an access by an access prohibited user listed on an access prohibition list; an input module is configured to input user information corresponding to the access prohibited user; and a list update module is configured to update the access prohibition list corresponding to each access controller connected with the network, according to the user information input through the input module;

a second feature of the present invention as recited in independent claim 9, wherein a receiving module is configured to receive user information of an access prohibited user, from another access controller; a list update module is configured to update an access prohibition list, which records user information of access prohibited users, according to the received user information; and an access interception module is configured to restrict the access by reference to the access prohibition list prior to the access control list;

a third feature of the present invention as recited in independent claim 15, wherein an access interception module is configured to restrict access by reference to an access prohibition list, which records user information of access prohibited users, prior to the access control list; at least one of the access controllers corresponding to an updated access prohibition list further comprises a distribution module configured to send out the user information or the updated access prohibition list to another access controller in response to the update; and the other access controller further comprises a list update module configured to receive the user information or the updated access prohibition list and to update the access prohibition list of the other access controller;

a fourth feature of the present invention as recited in independent claim 18, wherein an access interception module is configured to restrict access by reference to an access prohibition list, which records user information of access prohibited users, prior to the access control list; a distribution module is configured to broadcast the user information to another access controller in response to update of the own access prohibition list; a list update module is configured to update the access prohibition list in case of receiving the user information; an access control list update module is configured to update the access control list according to the user information after updating the access prohibition list; and a user information deletion module is configured to delete the user information from the access prohibition list after updating the access control list;

a fifth feature of the present invention as recited in independent claim 19, wherein in an access control method for controlling access to an information resource stored in a storage device, the method includes steps of intercepting an access by an access prohibited user listed on an access prohibition list; inputting user information corresponding to the access prohibited user; and updating the access prohibition list corresponding to each access controller connected with the network, according to the input user information;

a sixth feature of the present invention as recited in independent claim 20, wherein in an access control method for controlling access to an information resource stored in a storage device, the method includes steps of receiving user information of an access prohibited user from other access controller; updating an access prohibition list on which user information of access prohibited users is recorded, according to the received user information; and restricting the access by reference to the access prohibition list prior to the access control list;

a seventh feature of the present invention as recited in independent claim 21, wherein in an access control method for controlling access to information resources in an access control system, the method wherein each access controller restricts the access by reference to an access prohibition list, which records user information of access prohibited users, prior to the access control list; at least one of the access controllers corresponding to the updated access prohibition list sends out the user information or the updated access prohibition list to other access controller in response to the update; and the other access controller receives the user information or the updated access prohibition list and updates the access prohibition list of the other access controller;

an eighth feature of the present invention as recited in independent claim 22, wherein a computer readable recording medium contains a computer program executed by an access controller to control an access to an information resource stored in a storage device, the computer program comprising a second program code for intercepting an access by an access prohibited user listed on an access prohibition list; a third program code for inputting user information corresponding to the access prohibited user; and a fourth program code for updating the access prohibition list corresponding to each access controller connected with the network, according to the input user information; and

a ninth feature of the present invention as recited in independent claim 23, wherein a computer readable recording medium contains a computer program executed by an access controller to control an access to an information resource stored in a storage device, the computer program comprising a second program code for receiving user information of an access prohibited user from other access controller; a third program code for updating an access prohibition list on which user information of access prohibited users is recorded, according to the received user information; and a fourth program code for restricting the access according to the access prohibition list prior to the access control list.

To the extent applicable to the present Petition, Applicants submit that although the distinguishing features may represent a substantial portion of the claimed invention, the claimed invention including the features and their interoperation provides a novel access controller, method for access control, computer readable recording medium not taught or suggested by any of the references of record.

The references considered most closely related to the claimed invention are briefly discussed below:

Belani, et al., US 6,772,350 (Belani) discloses server control resources 18 with an access controller module ACLR 22. The ACLR 22 performs various functions and tasks for controlling access to the resources. A mechanism (for users) generates requests for access to resources 18. An access list information (associated with various resources) is stored in storage subsystem 32. Server 20 controls access to a particular resource based on the access list information. The operations on the resource may include update. (See, e.g., Abstract; column 5, lines 13-34; column 6, lines 3-13, lines 51-67; column 7, lines 1-18; and Figures 1-3).

Belani, however, does not disclose an access interception module configured to intercept an access by an access prohibited user listed on an access prohibition list.

More particularly, Belani does not teach or suggest the above-described first feature of the present invention as recited in independent claim 1, the above-described second feature of the present invention as recited in independent claim 9, the above-described third feature of the present invention as recited in independent claim 15, the above-described fourth feature of the present invention as recited in independent claim 18, the above-described fifth feature of the present invention as recited in independent claim 19, the above-described sixth feature of the present invention as recited in independent claim 20, the above-described seventh feature of the present invention as recited in independent claim 21, the above-described eighth feature of the present invention as recited in independent claim 22, and the above-described ninth feature of the present invention as recited in independent claim 23, in combination with the other limitations recited in each of the independent claims.

Nakamura, et al., US Patent Publication No. 2002/0053029 (Nakamura), discloses an access control server 200 having an access information database DB 209. A reception server 100 has a user profile 111, an access list 109 (holding access request information given from the users), an access information reporting part, an access registering part, a user authenticating part, and an access receiving part. A user transmits an access request for the service server 300 via a user terminal 50. (See, e.g., Abstract; paragraphs 58-60, 112-115, 122, 127, 129, 156; and Figures 1-9, 38.)

Nakamura, however, does not disclose a list update module configured to update the access prohibition list corresponding to each access controller connected with the network, according to the user information input through the input module.

More particularly, Nakamura does not teach or suggest the above-described first feature of the present invention as recited in independent claim 1, the above-described second feature of the present invention as recited in independent claim 9, the above-described third feature of the present invention as recited in independent claim 15, the above-described fourth feature of the present invention as recited in independent claim 18, the above-described fifth feature of the present invention as recited in independent claim 19, the above-described sixth feature of the present invention as recited in independent claim 20, the above-described seventh feature of the present invention as recited in independent claim 21, the above-described eighth feature of the present invention as recited in independent claim 22, and the above-described ninth feature of the present invention as recited in independent claim 23, in combination with the other limitations recited in each of the independent claims.

Dutta, et al., US Patent Publication No. 2002/0138727 (Dutta), discloses an authorization server 222. An interceptor 220 receives request to invoke a protected method and verifies the request should be granted or denied. An authorization process may use an access control list (ACL) authorization model. The authorization process dynamically consults the access control list (ACL) to determine whether a requesting module (client application) should be allowed to execute protected methods (supported on server 204). (See, e.g., Abstract; paragraphs 7, 14, 35-38, 43, 60, 62-63, 69, 70, 75, 77; and Figures 2-3.).

Dutta, however, does not disclose an input module configured to input user information corresponding to the access prohibited user. Furthermore, Dutta does not disclose a list update module configured to update the access prohibition list corresponding to each access controller connected with the network, according to the user information input through the input module.

More particularly, Dutta does not teach or suggest the above-described first feature of the present invention as recited in independent claim 1, the above-described second feature of the present invention as recited in independent claim 9, the above-described third feature of the present invention as recited in independent claim 15, the above-described fourth feature of the present invention as recited in independent claim 18, the above-described fifth feature of the present invention as recited in independent claim 19, the above-described sixth feature of the present invention as recited in independent claim 20, the above-described seventh feature of the present invention as recited in independent claim 21, the above-described eighth feature of the present invention as recited in independent claim 22, and the above-described ninth feature of the present invention as recited in independent claim 23, in combination with the other limitations recited in each of the independent claims.

Burnett, US Patent Publication No. 2003/0028798 (Burnett), discloses a security model with access control list (ACL). When a resource access occurs, an intercepting agent 40 (ACL manager) processes the access. The ACL manager determines whether the relevant protections are in the resource space for the accessed resource. The ACL manager gathers the access application restrictions. (See, e.g., Abstract; paragraphs 2, 4, 14, 15, 33, 35, 39-40, 47, 52; and Figures 1-2.)

Burnett, however, does not disclose an input module configured to input user information corresponding to the access prohibited user.

More particularly, Burnett does not teach or suggest the above-described first feature of the present invention as recited in independent claim 1, the above-described second feature of the present invention as recited in independent claim 9, the above-described third feature of the present invention as recited in independent claim 15, the above-described fourth feature of the present invention as recited in independent claim 18, the above-described fifth feature of the present invention as recited in independent claim 19, the above-described sixth feature of the present invention as recited in independent claim 20, the above-described seventh feature of the present invention as recited in independent claim 21, the above-described eighth feature of the present invention as recited in independent claim 22, and the above-described ninth feature of the present invention as recited in independent claim 23, in combination with the other limitations recited in each of the independent claims.

Hanson, et al., US Patent Publication No. 2004/0127190 (Hanson), discloses an access controller controls access to software services through an at least one interface. The access controller includes an interception module 223 (IM) for receiving a request the software services component. A security access manager 518 determines if a permission should be granted. The security access manager 518 (SAM) accesses an Access Control List (ACL) 312 to determine if permission should be granted. The SAM 518 distributes permission update requests to at least one IM 223 as required or at predetermined intervals. (See, e.g., Abstract; paragraphs 14, 16, 53-55, 63, 65-66, 68-69; and Figures 5-10.)

Hanson, however, does not disclose the list update module sends out other access controller a registration instruction to register the input user information on the access prohibition list of the other access controller.

More particularly, Hanson does not teach or suggest the above-described first feature of the present invention as recited in independent claim 1, the above-described second feature of the present invention as recited in independent claim 9, the above-described third feature of the present invention as recited in independent claim 15, the above-described fourth feature of the present invention as recited in independent claim 18, the above-described fifth feature of the present invention as recited in independent claim 19, the above-described sixth feature of the present invention as recited in independent claim 20, the above-described seventh feature of the present invention as recited in independent claim 21, the above-described eighth feature of the present invention as recited in independent claim 22, and the above-described ninth feature of the present invention as recited in independent claim 23, in combination with the other limitations recited in each of the independent claims.

Chebolu, et al., US Patent Publication No. 2005/0065935 (Chebolu), discloses an access control unit 155. A configuration profile (for each user) is going to be regulated by an administrator via the access control unit 155. A user command (to access a computer application) is intercepted in step 225. The access control unit 155 checks the configuration profile of a current user to determine whether the current is allowed to access a particular computer application. An I/O device 190 includes input devices. The configuration profiles (stored in a database) are updated with modified version. (See, e.g., Abstract; paragraphs 7, 39, 42, 46, 52, 54, 56, 62-65, 68-69, 71-72, 74-76, 80-82, 86-87, 91, 94; and Figures 1-3, 10-11.)

Chebolu, however, does not disclose the list update module sends out other access controller a registration instruction to register the input user information on the access prohibition list of the other access controller.

More particularly, Chebolu does not teach or suggest the above-described first feature of the present invention as recited in independent claim 1, the above-described second feature of the present invention as recited in independent claim 9, the above-described third feature of the present invention as recited in independent claim 15, the above-described fourth feature of the present invention as recited in independent claim 18, the above-described fifth feature of the present invention as recited in independent claim 19, the above-described sixth feature of the present invention as recited in independent claim 20, the above-described seventh feature of the present invention as recited in independent claim 21, the above-described eighth feature of the present invention as recited in independent claim 22, and the above-described ninth feature of the present invention as recited in independent claim 23, in combination with the other limitations recited in each of the independent claims.

Therefore, since the cited references fail to teach or the above-described first feature of the present invention as recited in independent claim 1, the above-described second feature of the present invention as recited in independent claim 9, and the above-described third feature of the present invention as recited in independent claim 15, the above-described fourth feature of the present invention as recited in independent claim 18, the above-described fifth feature of the present invention as recited in independent claim 19, the above-described sixth feature of the present invention as recited in independent claim 20, the above-described seventh feature of the present invention as recited in independent claim 21, the above-described eighth feature of the present invention as recited in independent claim 22, and the above-described ninth feature of the present invention as recited in independent claim 23, in combination with the other limitations recited in each of the independent claims, it is submitted that all of the claims are patentable over the cited references whether the references are taken individually or in combination with each other.

(F) Conclusion

Applicants have conducted what they believe to be a reasonable search, but make no representation that "better" or more relevant prior art does not exist. The United States Patent and Trademark Office is urged to conduct its own complete search of the prior art, and to thoroughly examine this application in view of the prior art cited herein and any other prior art that the United States Patent and Trademark Office may locate in its own independent search. Further, while Applicants have identified in good faith certain portions of each of the references listed herein in order to provide the requisite detailed discussion of how the claimed subject matter is patentable over the references, the United States Patent and Trademark Office should not limit its review to the identified portions but rather, is urged to review and consider the entirety of each reference, and not to rely solely on the identified portions when examining this application.

In view of the foregoing, Applicants request that this Petition to Make Special be granted and that the application undergo the accelerated examination procedure set forth in MPEP 708.02 VIII.

(G) Fee (37 C.F.R. 1.17(h))

The fee required by 37 C.F.R. § 1.17(h) is to be paid by:

[X] the Credit Card Payment Form (attached) for $130.00.

[ ] charging Account ____________ the sum of $130.00.

A duplicate of this petition is attached.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C., Deposit Account No. 50-1417 (MEI-101).

Respectfully submitted,

MATTINGLY, STANGER,
MALUR & BRUNDIDGE, P.C.

Daniel J. Stanger
Reg. No. 32,846

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Rd., Suite 370
Alexandria, Virginia 22314
(703) 684-1120
Date: July 29, 2005